Cours L3 2010 Christophe Certain

LES E-MAILS

Protocoles utilisés

- Envoi des mails : SMTP
  Transfert du m essage d'un point à un autre. Le message lui-même n'est pas traité
- Accès aux e-mails
  POP : permet de télécharger les e-mails du serveur (utilisation avec logiciels de messagerie comme Thunderbird (open source, suite Mozilla), Outlook (Microsoft) , Mail (Apple)
  IMAP : permet de gérer les e-mails directement sur le serveur et de les classer comme lus, mis à la corbeille, spams, etc. Ce protocole est utilisé pour les web-mails : Gmail, Hotmail, Yahoo, Free, ont des applications permettant la gestion des e-mails par web-mail.
  Important : IMAP laisse les messages intacts sur le serveur, POP télécharge les messages et les élimine ensuite sur le serveur. IMAP facilite donc la préservation des messages dans le temps, mais au prix d'un espace disque important sur le serveur. (Grâce à la politique de sauvegarde et de maintenance des hébergeurs, les données sont plus en sécurité chez l'hébergeur que chez vous)

Les utilisations des emails

A. **L'email : « one to one » et ses variantes « one to many »**
   - l'envoi avec « copie » le destinataire sait qu'une copie du document a été envoyée, on le fait généralement pour le montrer et se border dans l'éventualité de conflits éventuels. (ex. : envoie d'un mail à un client ou fournisseur et copie à son chef de service)
   - L'envoi en « copie cachée » est utilisé généralement pour envoyer un même message à plusieurs personnes ne se connaissant pas forcément entre elles. La netiquette recommande donc d'envoyer les messages en copie cachées, de façon à ce que les utilisateurs n'aient pas accès aux adresses e-mails de personnes qu'elles ne connaissent pas.
   - Le transfert ou « forward » permet de transférer un message reçu à une autre personne. Elle permet d'indiquer directement l'identité de la personne émettrice du message.
   - La demande d'accusé de réception : n'utiliser cette fonctionnalité qu'en cas de besoin réel, on la considère comme impolie sinon. De plus le récepteur n'est pas obligé de renvoyer l'accusé de réception pour accéder au mail.
   - **A éviter** : l'envoi de message à une liste de personnes directement dans le champ envoi, en séparant les emails par une virgule.
     - Les e-mails des personnes sont disséminées à des destinataires inconnus, ce qui peut entraîner :
       - des risques de réception de mails indésirables (« réponse à

tous » ou spammeur)
- des risques d'attaques de vers, trojan et virus en retour si l'une des machines réceptrices est infectée.

B. La newsletter : envoi d'e-mails « one to many » à sens unique

- On utilise la newsletter pour envoyer des informations à un groupe. La communication est à sens unique, seul le propriétaire de la newsletter peut envoyer des messages à l'ensemble des personnes abonnées à la liste. Un « répondre » au message n'enverra qu'un e-mail à la personne émettrice de la newsletter. La newsletter est un outil privilégié pour susciter un afflux de visiteurs sur le site web et déclencher la lecture de pages ou l'achat de produit. C'est un outil INDISPENSABLE. Suivant l'activité on pourra envoyer une news quotidienne (journal d'infos quotidien comme Slate.fr) hebdo, mensuelle et à l'occasion d'évènements particuliers : actualités, soldes, promotions, etc.
- Pour recevoir une newsletter il faut s'y abonner (formulaire avec adresse e-mail et prénom au minimum, ce qui permet de personnaliser les envois Bonjour %Prénom%) Dans certains cas les personnes sont abonnées d'office, il faut mieux cependant éviter l'envoi de mails non désirés (spam) et laisser le choix à la personne de recevoir ou non la newsletter (cas de nouveaux clients sur un site de vente en ligne ou service en ligne quelconque)
- Une newsletter doit toujours comprendre en bas du message la possibilité de se désabonner sous forme d'un lien vers un formulaire de désinscription. L'absence de ce type de lien suscite un fort mécontentement de la part de ceux qui ne souhaitent plus recevoir la news. Il y a pire que l'absence de lien : le lien de désabonnement qui ne marche pas. A vérifier donc, sous peine de vous faire des ennemis très remontés !
- **A éviter** : acheter des listes d'e-mails et spammer les gens avec la proposition de vos services en considérant que puisque vous avez acheté ces adresses, vous pouvez maintenant envoyer autant de mails que vous voulez. Cette attitude est contre-productive, car vous allez créer un très fort mécontentement chez ceux qui vont recevoir vos e-mails. Cela ne rapporte pas de clients (ou très peu) et nuit considérablement à l'image de la société. Le plus important est l'image de votre société sur le long terme.
- Jusqu'à 1000 abonnés, la gestion d'une newsletter peut se faire avec les outils courants et gratuits, la plupart du temps fournis par l'hébergeur (exemple OVH) ou de scripts basés sur PHP et Mysql. Au-delà, l'envoi massif d'e-mails nécessite d'être « white-listé » chez les gestionnaires de mails comme Hotmail, Gmail, etc. faute de quoi les e-mails n'arrivent jamais à destination car vous êtes considéré comme spammeur. Vos em-ilas peuvent également être reçus avec un ajout ***PROBABLY SPAM*** ou assimilé, qui fera que votre e-mail va aller directement dans le dossier « spams » ou « indésirable »
- Bien que la technologie permette d'envoyer des newsletter avec images, Flash, etc. Les newsletters qui génèrent le plus de retour sont les plus simples (texte uniquement). Il faut par contre soigner le texte (copy-writing) Chaque newsletter doit être rédigée. « Vous ne vendrez jamais un produit à un client que vous avez ennuyé ». Dans le cadre d'une démarche commerciale (vente en ligne) il est conseillé de travailler l'efficacité des textes en envoyant différentes versions d'un texte et en comparant les retombées (technique des coupons issue du marketing direct)
- Le taux d'ouverture moyen des newsletters est de 30% réparti sur plusieurs jours (ex. Cybermailing)
- mise en évidence du formulaire d'abonnement sur le site → taux de conversion
- calcul du taux de conversion
- renouvellement des adresses : « hard bounces » 0,5 à 0,7% par semaine (ex. Cybermailing)
- L'exemple de l'outil de gestion de newsletter professionnel Cybermailing

C. La liste de diffusion

- La liste de diffusion (mailing list) est liée à un groupe d'abonnés
- Chaque membre du groupe peut envoyer des e-mails à la liste
- Chaque e-mail envoyé à la liste est renvoyé automatiquement et individuellement à tous les abonnés du groupe (on n'a pas accès à l'ensemble de la liste des abonnés dans le champ adresse)
- On utilise la liste de diffusion pour la gestion des informations au sein d'un groupe (utilisateurs de logiciels ou de services, groupes de travail, etc.)
- Les listes peuvent être « ouvertes » ou « fermées » suivant qu'on peut s'y inscrire librement ou pas
- On peut généralement choisir la fréquence de réception des e-mails (quotidien ou digest hebdomadaire)
- Les listes de diffusion peuvent être gérée par un modérateur qui gère le spam, les trolls et les utilisateurs indésirables (indispensable quand la liste est « ouverte », c'est à dire quand n'importe qui peut s'abonner
- Les hébergeurs offrent généralement la possibilité de créer des listes de diffusion (ex.OVH)
- de nombreux sites offrent la possibilité de gérer gratuitement des listes de diffusion, avec une page web qui reprend l'ensemble des e-mails envoyés ex. le concept de « Google group » ou « Yahoo group »
- L'abonnement à une ou plusieurs listes de diffusion peut très rapidement encombrer votre boîte mail (plusieurs centaines d'e-mails par jour) il faut donc ne s'abonner qu'avec parcimonie et utiliser un logiciel de mail permettant de classer les mails par sujet (ex. Thunderbird)
- Un envoi de mail au robot qui gère la liste de diffusion avec comme sujet « subscribe » ou « unsubscribe » suffit généralement pour s'abonner ou se désabonner de la liste. Les explications pour s'abonner ou se désabonner doivent être clairement accessibles pour les utilisateurs.

D. Les répondeurs

- Les hébergeurs laissent généralement la possibilité de créer des répondeurs automatiques. Quand un message est envoyé à une certaine adresse par un internaute, celui-ci reçoit automatiquement une réponse prédéterminée, de façon temporaire ou définitive
  Ex.temporaire : M. Untel est absent du XX/XX/2010 au XX/XX/2010 merci de vous adresser à Mme Dupont dupont@dupont.com en son absence
  Ex. définitif : Mme Dugenou est partie à la retraite, cette adresse e-mail n'est plus valide.

E. Les « catch all »

- Le catch all est une adresse qui permet de récupérer l'ensemble des e-mails envoyés à un nom de domaine, erreurs d'adresses comprises.
  Par exemple : jean.dupont@dupont.com arrive normalement à son destinataire mais jean.dupond@dupont.com ou jan.dupont@dupont.com n'arriveront pas à leur destinataire à cause d'une erreur dans l'adresse. Ils seront cependant récupérés par le catch all, dans la mesure où le nom de domaine est correct.
- Les catch all sont cependant de moins en moins utilisés en raison du trop grand nombre de spam puisque nimportequoi@dupont.com est récupéré par le catch all

F. Les redirections d'e-mail

- Les redirections sont utilisées pour éviter d'avoir plusieurs comptes e-mails à gérer. Elles sont généralement mises à disposition par l'hébergeur (ex. OVH)
- On indique l'adresse de réception des courriels, et l'adresse vers laquelle les courriels doivent être redirigés.

G. Antispam et antivirus pour e-mails

- Les logiciels d'e-mails peuvent être sensibles aux virus (Outlook par exemple) mais les e-mails peuvent également véhiculer en pièce jointe d'autres nuisances comme des vers ou des trojans. Il est donc formellement déconseillé d'ouvrir des pièces jointes si vous ne connaissez pas la provenance de l'expéditeur, et ce quel que soit le contenu supposé de la pièce jointe (ex. « I love you »)
- Les e-mails sont également sujets au SPAM c'est à dire l'envoi de mails non désirés. 60% de l'ensemble du trafic du web serait causé par les envois de spams. Ils sont donc une calamité pour l'ensemble des utilisateurs du web
- Une protection résidente (ex. Avast) sur votre ordinateur permet de déceler les e-mails porteurs de virus vers ou trojans
- Une protection est parfois aussi offerte par l'hébergeur (ex. OVH)
- Concernant le spam, des règles peuvent être configurées sur votre logiciel d'e-mail
- Une protection peut également être installée au niveau du serveur (ex. OVH)
- Le fait d'avoir une protection anti-spam nécessite d'aller vérifier régulièrement le contenu de la boîte « indésirables » afin de vérifier que des mails important n'ont pas été jetés dans cette boîte (cela arrive régulièrement donc attention!)